UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/708,988	04/06/2004	Wen-Long Chin	ADMP0002USA	2987

27765 7590 05/07/2007
NORTH AMERICA INTELLECTUAL PROPERTY CORPORATION
P.O. BOX 506
MERRIFIELD, VA 22116

EXAMINER
DEBNATH, SUMAN

ART UNIT	PAPER NUMBER
2135	

NOTIFICATION DATE	DELIVERY MODE
05/07/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

winstonhsu.uspto@gmail.com
Patent.admin.uspto.Rcv@naipo.com
mis.ap.uspto@naipo.com.tw

Office Action Summary	Application No.	Applicant(s)	
	10/708,988	CHIN ET AL.	
	Examiner	Art Unit	
	Suman Debnath	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 April 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-21 are pending in this application.

2. Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nakanishi (Patent Number: 5,805,852) in view of Crispin et al. (Pub. No.: US 2004/0228479 A1), hereinafter "Crispin"

5. As to claim 1, Nakanishi discloses a method by using a very long instruction word (VLIW) architecture processor (column 8, lines 55-60), the processor comprising:

a buffer for storing data (column 9, lines 15-25 and lines 50-65);

a first register electrically connected to the buffer having a plurality of output ports and a plurality of input ports (column 9, lines 28-65);

an input/output (I/O) controller electrically connected to the buffer and the first register for controlling data to be transmitted from the first register to the buffer or from the buffer to the first register (column 3, lines 39-65 and column 10, lines 60-67);

an arithmetic logic unit (ALU) (column 10, lines 10-30) comprising:

a plurality of input ports (column 10, lines 10-30);

a plurality of output ports (column 10, lines 10-30);

a basic logic operation unit for executing basic logic operations (column 5, lines 11-45 and column 10, lines 10-30); and

a plurality of multiplexers each having a plurality of input ports electrically connected to the output port of the first register or the output port of the ALU, and one output port electrically connected to the output port of the ALU and the output port of the first register (column 3, lines 19-65);

a command input port; a command register electrically connected to the command input port for temporarily storing the commands input to the command input port (column 9, lines 1-13); and

a command decoder/scheduler electrically connected to the command register, the plurality of multiplexers, and the ALU for decoding and scheduling the commands

from the command register in order to control at least one of the multiplexers to output and input one of the plurality of data units stored in the multiplexer to the ALU and control the ALU to operate (column 9, lines 15-65 and column 10, lines 60-67), the method comprising:

(b) sending the command stored in the command input port to the command register (column 9, lines 1-13);

(c) sending the command input into the command register to the command decoder/scheduler (column 9, lines 15-65 and column 10, lines 60-67);

(d) decoding and scheduling the command sent from the command register to the command decoder/scheduler (column 9, lines 15-65 and column 10, lines 60-67);

(e) controlling at least one of the multiplexers to output one of the plurality of data units input into the multiplexer from the first register and the ALU to the ALU and the first register, and controlling the ALU to operate (column 3, lines 39-65 and column 10, lines 60-67); and

(f) inputting data generated by the operation of the ALU into the plurality of multiplexers (column 3, lines 39-52, column 9, lines 15-65 and column 10, lines 60-67).

Nakanishi doesn't explicitly disclose for implementing advanced encryption standards (AES). A special AES command unit for executing special logic operations according to AES. Receiving commands of AES execution. (a) inputting the command of AES execution into the command input port.

However, Crispin discloses for implementing advanced encryption standards (AES) (FIG. 12, [0009], [0010]). A special AES command unit for executing special

logic operations according to AES ([0023] – [0024], [0069]). Receiving commands of AES execution ([0023] – [0024], [0069]). (a) inputting the command of AES execution into the command input port ([0023] – [0024], [0037], [0069]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Nakanishi as taught by Crispin in order to provide "concurrent cryptographic operations". (Crispin)

6. As to claim 2, Nakanishi doesn't explicitly disclose processing and executing commands for a plurality of different modes according to AES. However, Crispin discloses processing and executing commands for a plurality of different modes according to AES ([0012]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Nakanishi as taught by Crispin in order to provide wide verity of applications.

7. As to claim 3, Nakanishi doesn't explicitly disclose executing 128-bit, 192-bit, 256-bit AES (AES-128, AES-192, AES-256) encryption/decryption. However, Crispin discloses executing 128-bit, 192-bit, 256-bit AES (AES-128, AES-192, AES-256) encryption/decryption ([0009] – [0010]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Nakanishi as taught by Crispin in order to provide wide verity of applications.

8. As to claim 4, Nakanishi discloses wherein the first register comprises a plurality of registers including register R0, register R1, register R2 and register R3, and simultaneously process the least significant byte (LSB) and the second least significant byte counted for 8 bytes stored in register R0, register R1, register R2, register R3 (column 9, lines 1-13, column 1, lines 29-35, column 2, lines 10-45, column 13, lines 1-40). Nakanishi doesn't explicitly disclose a method that is able to execute an SBSR1 (substitute byte shift row 1) command. However, Crispin discloses a method that is able to execute an SBSR1 (substitute byte shift row 1) command ([0010]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Nakanishi as taught by Crispin in order to provide "concurrent cryptographic operations". (Crispin)

9. As to claim 5, Nakanishi discloses simultaneously process the most significant byte (MSB) and the second most significant byte counted for 8 bytes stored in register R0, register R1, register R2, and register R3 (column 9, lines 1-13, column 1, lines 29-35, column 2, lines 10-45, column 13, lines 1-40). Nakanishi doesn't explicitly disclose a method that is able to execute an SBSR2 (substitute byte shift row 1) command. However, Crispin discloses a method that is able to execute an SBSR2 (substitute byte shift row 1) command ([0010]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Nakanishi as taught by Crispin in order to provide "concurrent cryptographic operations". (Crispin)

10. As to claim 6, Nakanishi discloses wherein the first register comprises a plurality of registers including register R0, register R1, register R2 and register R3, command and simultaneously process data stored in register R0 and register R1 (column 9, lines 1-13, column 1, lines 29-35, column 2, lines 10-45, column 13, lines 1-40).

Nakanishi doesn't explicitly disclose executing an MIXADK1 (mix column add round key 1). However, Crispin discloses executing an MIXADK1 (mix column add round key 1) ([0010], "AddRoundKey").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Nakanishi as taught by Crispin in order to provide "concurrent cryptographic operations". (Crispin)

11. As to claim 7, Nakanishi discloses wherein simultaneously process data stored in register R2 and register R3 (column 9, lines 1-13, column 1, lines 29-35, column 2, lines 10-45, column 13, lines 1-40). Nakanishi doesn't explicitly disclose executing an MIXADK2 command. However Crispin discloses executing an MIXADK2 command ([0010]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Nakanishi as taught by Crispin in order to provide "concurrent cryptographic operations". (Crispin)

12. As to claims 8 and 9, Nakanishi doesn't explicitly disclose being able to simultaneously generating an AES encryption key and encrypt a plain text according to AES. However, Crispin discloses being able to simultaneously generating an AES encryption key and encrypt a plain text according to AES ([0010], [0023] – [0024], [0037], [0069]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Nakanishi as taught by Crispin in order to provide "concurrent cryptographic operations". (Crispin)

13. As to claim 10, Nakanishi discloses wherein the first register comprises a plurality of registers including register R0, register R1, register R2, and register R3, and simultaneously process the LSB and the second least significant byte counted for 8 bytes stored in register R0, register R1, register R2, and register R3 (column 9, lines 1-13, column 1, lines 29-35, column 2, lines 10-45, column 13, lines 1-40). Nakanishi doesn't explicitly disclose and the method is able to execute an INVSBSR1 (inverse substitute byte shift row 1) command.

However, Crispin discloses a method executing an INVSBSR1 (inverse substitute byte shift row 1) command ([0010]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Nakanishi as taught by Crispin in order to provide "concurrent cryptographic operations". (Crispin)

14. As to claim 11, Nakanishi discloses simultaneously process the MSB and the second most significant byte counted for 8 bytes stored in register R0, register R1, register R2, and register R3 (column 9, lines 1-13, column 1, lines 29-35, column 2, lines 10-45, column 13, lines 1-40). Nakanishi doesn't explicitly disclose being able to execute an INVSBSR2 command. However, Crispin discloses being able to execute an INVSBSR2 command ([0010]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Nakanishi as taught by Crispin in order to provide "concurrent cryptographic operations". (Crispin)

15. As to claim 12, Nakanishi discloses wherein the first register comprises a plurality of registers including register R0, register R1, register R2 and register R3, and simultaneously process data stored in register R0 and register R1 (column 9, lines 1-13, column 1, lines 29-35, column 2, lines 10-45, column 13, lines 1-40). Nakanishi doesn't explicitly disclose a method is able to execute an INVMIXADK1 (inverse mix column add round key 1) command. However, Crispin discloses a method is able to execute an INVMIXADK1 (inverse mix column add round key 1) command ([0010]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Nakanishi as taught by Crispin in order to provide "concurrent cryptographic operations". (Crispin)

16. As to claim 13, it is rejected using the same rationale as for the rejection of claim 12.

17. As to claim 14, Nakanishi discloses wherein the first register comprises a plurality of registers including register R20, register R21, register R22 and register R23, and simultaneously process the LSB and the second least significant byte counted for 8 bytes stored in register R20, register R21, register R22, and register R23 (column 9, lines 1-13, column 1, lines 29-35, column 2, lines 10-45, column 13, lines 1-40). Nakanishi doesn't explicitly disclose a method that is able to execute an SBSR3 command. However, Crispin discloses a method that is able to execute an SBSR3 command ([0010]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Nakanishi as taught by Crispin in order to provide "concurrent cryptographic operations". (Crispin)

18. As to claim 15, Nakanishi discloses method for simultaneously processing the MSB and the second most significant byte counted for 8 bytes stored in register R20, register R21, register R22, and register R23 (column 9, lines 1-13, column 1, lines 29-

35, column 2, lines 10-45, column 13, lines 1-40). Nakanishi doesn't explicitly disclose a method that is able to execute an SBSR4 command. However, Crispin discloses a method that is able to execute an SBSR4 command ([0010]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Nakanishi as taught by Crispin in order to provide "concurrent cryptographic operations". (Crispin)

19. As to claim 16, Nakanishi discloses wherein the first register comprises a plurality of registers including register R20, register R21, register R22 and register R23, and simultaneously process data stored in register R20 and register R21 (column 9, lines 1-13, column 1, lines 29-35, column 2, lines 10-45, column 13, lines 1-40). Nakanishi doesn't explicitly disclose a method that is able to execute an MIXADK3 command. However, Crispin discloses a method that is able to execute an MIXADK3 command ([0010]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Nakanishi as taught by Crispin in order to provide "concurrent cryptographic operations". (Crispin)

20. As to claim 17, it is rejected using the same rationale as for the rejection of claim 16.

21. As to claim 18, Nakanishi discloses wherein the first register comprises a plurality of registers including register R20, register R21, register R22 and register R23, and simultaneously process the LSB and the second least significant byte counted for 8 bytes stored in register R20, register R21, register R22, and register R23 (column 9, lines 1-13, column 1, lines 29-35, column 2, lines 10-45, column 13, lines 1-40). Nakanishi doesn't explicitly disclose a method that is able to execute an INVSBSR3 command. However, Crispin discloses a method that is able to execute an INVSBSR3 command ([0010]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Nakanishi as taught by Crispin in order to provide "concurrent cryptographic operations". (Crispin)

22. As to claim 19, Nakanishi discloses simultaneously processing the MSB and the second most significant byte counted for 8 bytes stored in register R20, register R21, register R22, and register R23 (column 9, lines 1-13, column 1, lines 29-35, column 2, lines 10-45, column 13, lines 1-40). Nakanishi doesn't explicitly disclose being able to execute an INVSBSR4 command. However, Crispin discloses being able to execute an INVSBSR4 command ([0010]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Nakanishi as taught by Crispin in order to provide "concurrent cryptographic operations". (Crispin)

23. As to claim 20, Nakanishi doesn't explicitly disclose being able to execute AES encryption/decryption in OCB (offset code book) mode and CCM (counter mode with CBC MAC) mode. However, Crispin discloses being able to execute AES encryption/decryption in OCB (offset code book) mode and CCM (counter mode with CBC MAC) mode ([0012]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Nakanishi as taught by Crispin in order to provide "concurrent cryptographic operations". (Crispin)

24. As to claim 21, Nakanishi doesn't explicitly disclose being able to use the same encryption key to simultaneously encrypt a plurality of data units. However, Crispin discloses being able to use the same encryption key to simultaneously encrypt a plurality of data units ([0010], [0017], [0040]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Nakanishi as taught by Crispin in order to provide "concurrent cryptographic operations". (Crispin)

Conclusion

25. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See accompanying PTO 892.

- US 2004/0146158 A1 – Cryptographic systems and methods supporting multiple modes.

- US 2004/0202317 A1-AES implementation as an instruction set extension.

26. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Suman Debnath whose telephone number is 571 270 1256. The examiner can normally be reached on 8 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

SD

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100